Original document

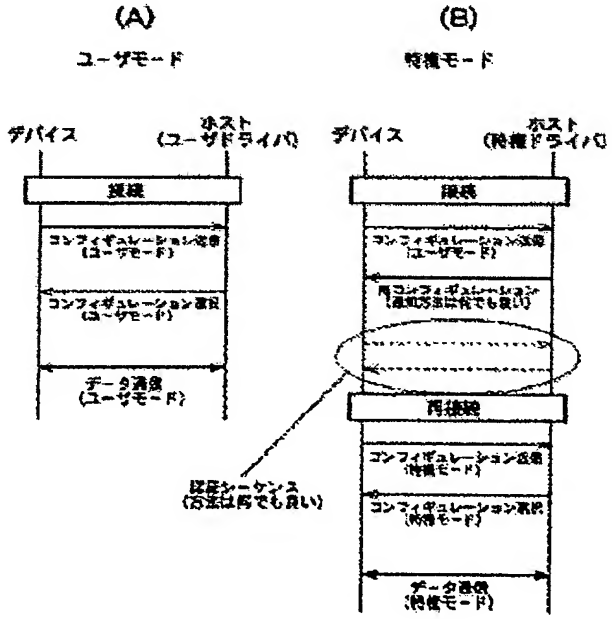
INITIALIZATION METHOD AND UBS DRIVER

Publication number: JP2004094514
Publication date: 2004-03-25
Inventor: NUNOURA TAKEFUMI; YAMAMOTO HIROSHI; SUZUKI MASANORI; MORIMOTO MASASHI; SHIOBARA TETSUYA
Applicant: JAPAN RADIO CO LTD
Classification:
- international: ***G06F13/14; G06F13/38;*** **G06F13/14; G06F13/38;** (IPC1-7): G06F13/14; G06F13/38
- European:
Application number: JP20020253754 20020830
Priority number(s): JP20020253754 20020830

View INPADOC patent family
View list of citing documents

Report a data error here

Abstract of **JP2004094514**
PROBLEM TO BE SOLVED: To prevent a privilege mode from being inferred by a general user.
SOLUTION: Configuration data for the general user are transmitted in a device side to conduct data communication by a user mode when a configuration thereof is selected (A). When the configuration thereof is not selected, a configuration data for a privilege user is transmitted after an authentication procedure or the like to conduct data communication by a privileged mode when a configuration thereof is selected (B). A host concerned in the general user selects the configuration data for the general user (A), and a host concerned in the privileged user requires reconfiguration to try reconnection by the configuration data for the privileged user (B).



JP2004094514: No description available

Data supplied from the ***esp@cenet*** database - Worldwide

JP2004094514: No claims available

Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-94514
(P2004-94514A)
(43)公開日　平成16年3月25日(2004.3.25)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 13/14	G06F 13/14	330A	5B014
G06F 13/38	G06F 13/38	350	5B077

審査請求 有　請求項の数 6　OL　（全 13 頁）

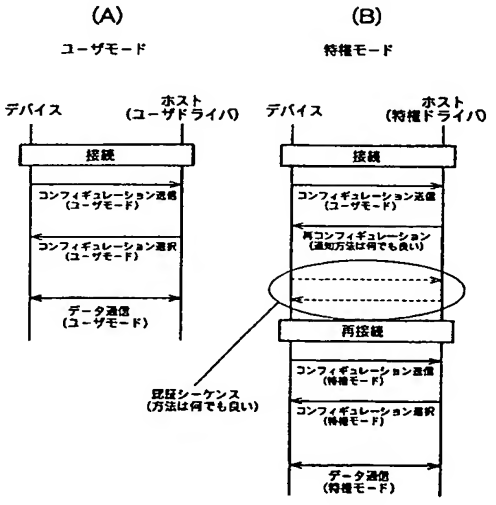
(21)出願番号　特願2002-253754(P2002-253754)
(22)出願日　平成14年8月30日(2002.8.30)

(71)出願人　000004330
日本無線株式会社
東京都三鷹市下連雀５丁目１番１号
(74)代理人　100075258
弁理士　吉田　研二
(74)代理人　100096976
弁理士　石田　純
(72)発明者　布浦　武文
東京都三鷹市下連雀五丁目１番１号　日本無線株式会社内
(72)発明者　山本　弘
東京都三鷹市下連雀五丁目１番１号　日本無線株式会社内

最終頁に続く

(54)【発明の名称】初期化方法及びＵＳＢドライバ

(57)【要約】
【課題】特権モードが一般ユーザに察知されないようにする。
【解決手段】デバイス側では、一般ユーザ向けのコンフィギュレーションデータを送信して、そのコンフィギュレーションが選択されたらユーザモードでのデータ通信を行う（A）。逆に、そのコンフィギュレーションが選択されなかった場合は、認証手順等を経た上で、特権ユーザ向けのコンフィギュレーションデータを送信して、そのコンフィギュレーションが選択されたら特権モードでのデータ通信を行う（B）。一般ユーザに係るホストが、一般ユーザ向けのコンフィギュレーションデータを選択するのに対し（A）、特権ユーザに係るホストは、再コンフィギュレーションを要求して、特権ユーザ向けのコンフィギュレーションデータによる再接続を試行する（B）。
【選択図】　図3



【特許請求の範囲】
【請求項１】
ＵＳＢデバイスの機能構成を示すコンフィギュレーションデータをＵＳＢデバイスからＵＳＢホストへと送信するステップ及びこの送信への応答としてＵＳＢホストからＵＳＢデバイスにＵＳＢ通信開始許可又は拒否を通知するステップを含む初期化手順を、ＵＳＢデバイスをＵＳＢホストに接続する際にＵＳＢデバイス・ＵＳＢホスト間通信により実行する初期化方法において、ＵＳＢホストからＵＳＢ通信開始拒否が通知されたときに、先に送信したコンフィギュレーションデータにより特定される機能構成とは別の機能構成を示す他のコンフィギュレーションデータをＵＳＢデバイスから送信することによって、初期化手順を再実行させることを特徴とする初期化方法。
【請求項２】
請求項１記載の初期化方法において、
初期化手順の再実行を、ＵＳＢホストからＵＳＢデバイスへとＵＳＢ通信開始許可が通知されるまで、また使用するコンフィギュレーションデータを逐次変更しつつ、所定回数を限度として繰り返すことを特徴とする初期化方法。
【請求項３】
請求項１又は２記載の初期化方法において、
初期化手順を再実行する際に、コンフィギュレーションデータの送信に先立ち、ＵＳＢデバイス・ＵＳＢホスト間通信により、ＵＳＢデバイスがＵＳＢホストを認証するため又はＵＳＢデバイス・ＵＳＢホスト間の相互認証のための認証手順を実行することを特徴とする初期化方法。
【請求項４】
請求項１乃至３のいずれか一項記載の初期化方法において、最初に実行される初期化手順にて送受信されるコンフィギュレーションデータが、一般ユーザ向けのコンフィギュレーションデータであり、
再実行に係る初期化手順にて送受信されるコンフィギュレーションデータが、一般ユーザとは異なる権限を有する特権ユーザ向けのコンフィギュレーションデータであることを特徴とする初期化方法。
【請求項５】
請求項４記載の初期化方法を実行するためＵＳＢデバイスにインストールされるデバイス側ＵＳＢドライバにおいて、
上記ＵＳＢデバイスがＵＳＢホストに接続されたときに、そのＵＳＢホストに対し上記ＵＳＢデバイスの機能構成を示しかつ一般ユーザ向けのコンフィギュレーションデータを送信し、それに対する応答としてＵＳＢ通信開始許可が通知された場合に、接続先のＵＳＢホストとのデータ通信を開始させ、
接続先のＵＳＢホストからＵＳＢ通信開始拒否が通知された場合に、接続先のＵＳＢホストが特権ユーザに係るホストであると見なし、そのＵＳＢホストに対し特権ユーザ向けのコンフィギュレーションデータを送信して、ＵＳＢ通信開始許可を求めることを特徴とするデバイス側ＵＳＢドライバ。
【請求項６】
請求項５記載のデバイス側ＵＳＢドライバがインストールされたＵＳＢデバイスが接続されるＵＳＢホストに、請求項４記載の初期化方法を実行するため、インストールされるホスト側ＵＳＢドライバにおいて、
新たに接続されたＵＳＢデバイスからそのＵＳＢデバイスの機能構成を示すコンフィギュレーションデータを受信した場合に、そのコンフィギュレーションデータに関しては一般ユーザ向けのコンフィギュレーションデータであると見なし、送信元のＵＳＢデバイスに対しＵＳＢ通信開始拒否を通知し、
通知先のＵＳＢデバイスから前回とは異なるコンフィギュレーションデータを受信した場合に、そのコンフィギュレーションデータに関しては特権ユーザ向けのコンフィギュレーションデータであると見なし、ＵＳＢ通信開始許可及び拒否のいずれかを通知することを

特徴とするホスト側ＵＳＢドライバ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）デバイスをＵＳＢホストに接続したときに実行される初期化方法、並びにこの初期化方法の実施に適するＵＳＢドライバに関する。
【０００２】
【従来の技術】
ＵＳＢデバイス（以下単に「デバイス」）をＵＳＢホスト（以下単に「ホスト」）例えばＰＣに接続する際には、デバイス・ホスト間通信により初期化（エニュメレーション）手順が実行される。初期化手順においては、デバイスの機能構成即ちコンフィギュレーションを示すコンフィギュレーションデータが、デバイスからホストへと送信される（コンフィギュレーション送信）。その際、複数通りのコンフィギュレーションデータをデバイスからホストへと送信することもできる。ホストは、受信したコンフィギュレーションデータの中から、そのデータにより特定されるコンフィギュレーション下でのデータ通信を許可できるものを選択して、その結果をデバイスに通知する（コンフィギュレーション選択）。これらのステップを含む初期化手順を経た上で、デバイス・ホスト間で、ＵＳＢインタフェースによるデータ通信が開始される。なお、受信したコンフィギュレーションデータにより特定されるコンフィギュレーション（群）のなかに、データ通信開始を許可できるコンフィギュレーションが見あたらない場合、ホストはデータ通信を拒否する。
【０００３】
また、複数通りのコンフィギュレーションをとりうるデバイスをホストに接続する際には、例えば、上述の通り、各コンフィギュレーションに対応する合計複数通りのコンフィギュレーションデータがデバイスからホストに送信される。目的・用途によっては、複数通りのコンフィギュレーションデータのうち一つにより初期化手順が実行され、その結果に応じて他のコンフィギュレーションデータにより初期化手順が実行されることもある。例えば、下記特許文献１に記載のデバイスでは、デバイスからホストへのソフトウエア類（ドライバ、ユーティリティ等）の転送に適する第１のコンフィギュレーションと、通常のデータ転送に適する第２のコンフィギュレーションとが、準備されている。デバイスをホストに接続すると、第１のコンフィギュレーションを示すコンフィギュレーションデータがホストに送られ、このコンフィギュレーションデータ中に含まれている識別情報等に従ってホストがデバイスからドライバ等を受信及びインストールする。その後、第２のコンフィギュレーションを示すコンフィギュレーションデータがホストに送られ、適宜、データ通信が開始される。従って、デバイスをホストに接続するだけで、そのデバイス用のドライバ、ユーティリティ等の更新版をホストに自動インストールできる。
【特許文献１】
特開２０００－１９４６４５号公報
【０００４】
【発明が解決しようとする課題】
デバイスに複数通りのコンフィギュレーションを設ける目的としては、上掲のインストール自動化の他に、ユーザ種別によるコンフィギュレーションの切替等がある。ここでいうユーザ種別とは、そのデバイスをその本来用途通りに使用する一般ユーザ、一般ユーザとは異なる権限を有する特権ユーザ等の区別のことである。ＵＳＢポートを有する通信端末を例とすると、ＵＳＢポートを有するＰＣ等にその通信端末をＵＳＢ接続して通信を行うユーザが、一般ユーザに該当する。これに対して、その通信端末の保守、点検等のサービスを行う者のように、一般ユーザとは異なる目的及び権限でその通信端末を使用する者が、特権ユーザに該当する。一般ユーザと特権ユーザの権限は、例えば、デバイス内に格納されている情報、特に秘密保持義務が課されている情報に対するアクセス権等において、相違している。具体的には、漏洩することを防ぐべき個人情報等に対しては、特権ユーザ

はアクセスできても一般ユーザはアクセスできないようにすべきである。

【０００５】

こういった目的を達成するための一手法として、一般ユーザ向けのコンフィギュレーションと特権ユーザ向けのコンフィギュレーションを個々別々に準備する、という手法がある。その場合、図１２に示すように、デバイスをホストに接続した直後に、一般ユーザ向けのコンフィギュレーションデータ及び特権ユーザ向けのコンフィギュレーションデータを、デバイスからホストに送信する。これら２通りのコンフィギュレーションデータを受信したホスト、具体的にはそのホストで使用しているＵＳＢドライバ（以下単に「ドライバ」）は、それらのうち一方を選択する。例えば、一般ユーザ向け即ち通常のデータ通信のドライバであるユーザドライバはインストールされているが、特権ユーザ向け即ち保守等の特殊用途向けのドライバである特権ドライバはインストールされていない、というホストにおいては、図１２（Ａ）に示すように、一般ユーザ向けのコンフィギュレーションが選択され、そのコンフィギュレーション下でのデータ通信即ちユーザモードでのデータ通信が実行される。これに対して、特権ドライバがインストールされているＵＳＢホストにおいては、図１２（Ｂ）に示すように、特権ユーザ向けのコンフィギュレーションが選択され、そのコンフィギュレーション下でのデータ通信即ち特権モードでのデータ通信が実行される。

【０００６】

このようにすれば、一般ユーザと特権ユーザの別に応じて、デバイスのコンフィギュレーションを切り替えてデータ通信を行うことができる。しかしながら、図１２に示した手法では、ＵＳＢの規格・仕様に倣い、一般ユーザ向け及び特権ユーザ向けの合計２通りのコンフィギュレーションデータを同時一括送信し、ホスト側でコンフィギュレーション選択を行っている。これは、初期化シーケンスを実行し始める時点ではホストのユーザが一般か特権かをデバイスで認識できていないためであり、従来型の手順の単純応用では余儀なくされる措置であるけれども、反面、一般ユーザが使用しているホストが特権モードの存在を知ってしまうという問題を生じさせる。特権モードの存在が知られるということは、例えば、デバイス内に格納されておりユーザモードではアクセスできない情報にアクセスするための迂路の存在が、一般ユーザに知られうる、ということである。技術力と悪意又は遊戯心を持ったユーザならば、この迂路を通じて個人情報を入手することや、特権モード用のコンフィギュレーションデータと上掲の迂路を通じて入手した情報に基づき特権ドライバを自前で作成すること等が、可能である。一般ユーザ向け及び特権ユーザ向けの合計２通りのコンフィギュレーションデータを同時一括送信することには、このような情報セキュリティ面での問題を含め、いくつかの問題がある。

【０００７】

本発明の目的の一つは、初期化シーケンスを特権ユーザ以外に特権モードの存在が察知されにくい手順にすること、またそれに適するドライバを提供することにある。

【０００８】

【課題を解決するための手段】

このような目的を達成するために、本発明は、（１）デバイスの機能構成を示すコンフィギュレーションデータをデバイスからホストへと送信するステップ及びこの送信への応答としてホストからデバイスにＵＳＢ通信開始許可又は拒否を通知するステップを含む初期化手順を、デバイスをホストに接続する際にデバイス・ホスト間通信により実行する初期化方法において、（２）ホストからＵＳＢ通信開始拒否が通知されたときに、先に送信したコンフィギュレーションデータにより特定される機能構成とは別の機能構成を示す他のコンフィギュレーションデータをデバイスから送信することによって、初期化手順を再実行させることを特徴とする。より好ましくは、（３）初期化手順の再実行を、ホストからデバイスへとＵＳＢ通信開始許可が通知されるまで、また使用するコンフィギュレーションデータを逐次変更しつつ、所定回数を限度として繰り返すこととする。更に好ましくは、（４）初期化手順を再実行する際に、コンフィギュレーションデータの送信に先立ち、デバイス・ホスト間通信により、デバイスがホストを認証するため又はデバイス・ホスト

間の相互認証のための認証手順を実行することとする。また、例えば、（５）最初に実行される初期化手順にて送受信されるコンフィギュレーションデータは、一般ユーザ向けのコンフィギュレーションデータであり、（６）再実行に係る初期化手順にて送受信されるコンフィギュレーションデータは、一般ユーザとは異なる権限を有する特権ユーザ向けのコンフィギュレーションデータであるものとする。

【０００９】

また、本発明は、（７）上掲の認証機能を備え一般ユーザ向け及び特権ユーザ向けにそれぞれコンフィギュレーションデータが準備されたデバイスにインストールされるデバイス側ドライバにおいて、（８）上記デバイスがホストに接続されたときに、そのホストに対し上記デバイスの機能構成を示しかつ一般ユーザ向けのコンフィギュレーションデータを送信し、それに対する応答としてＵＳＢ通信開始許可が通知された場合に、接続先のホストとのデータ通信を開始させ、（９）接続先のホストからＵＳＢ通信開始拒否が通知された場合に、接続先のホストが特権ユーザに係るホストであると見なし、そのホストに対し特権ユーザ向けのコンフィギュレーションデータを送信して、ＵＳＢ通信開始許可を求めることを特徴とする。本発明は、（１０）上掲のデバイス側ドライバがインストールされたデバイスが接続されるホストにインストールされるホスト側ドライバにおいて、（１１）新たに接続されたデバイスからそのデバイスの機能構成を示すコンフィギュレーションデータを受信した場合に、そのコンフィギュレーションデータに関しては一般ユーザ向けのコンフィギュレーションデータであると見なし、送信元のデバイスに対しＵＳＢ通信開始拒否を通知し、（１２）通知先のデバイスから前回とは異なるコンフィギュレーションデータを受信した場合に、そのコンフィギュレーションデータに関しては特権ユーザ向けのコンフィギュレーションデータであると見なし、ＵＳＢ通信開始許可及び拒否のいずれかを通知することを特徴とする。

【００１０】

【発明の実施の形態】

以下、本発明の好適な実施形態に関し図面に基づき説明する。

【００１１】

図１及び図２に本発明の実施環境の一例を示す。これらの図のうち、図１に示したのはハードウエア構成、図２に示したのはソフトウエア構成である。本発明は、これらの図に示されているように、ＰＨＳ端末等のデバイス１０と、ＰＣ等のホスト２０とを、ＵＳＢケーブルにて接続したシステム環境にて実施可能である。

【００１２】

また、デバイス１０は、ＭＰＵ１１、ＲＡＭ１２、ＲＯＭ１３、クロック発生部１４、ＵＳＢコントローラ１５等のハードウエアを有している。アプリケーションプログラム１００やドライバ１０１等のソフトウエア類や、それらのソフトウエアにより使用されるデータ例えばコンフィギュレーションデータは、例えばＲＯＭ１３に予め書き込んでおく。ＭＰＵ１１は、ＲＡＭ１２によって提供される記憶空間を利用してそれらのソフトウエアに従い処理を実行し、デバイス１０全体の動作を制御・管理する。クロック発生部１４は、デバイス１０の動作速度を規定するクロックを発生させる。ＵＳＢコントローラ１５は、ＵＳＢ接続のためのハードウエアである。

【００１３】

アプリケーションプログラム１００は、ドライバ１０１を介してＵＳＢを使用する。ドライバ１０１は、ＡＰＩ（ＡＰＰｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍｉｎｇ Ｉｎｔｅｒｆａｃｅ）１０２、通信制御１０３、プロトコル制御１０４、認証処理１０５等のモジュールにより構成されている。ＡＰＩ１０２は、アプリケーションプログラム１００やその実行環境であるＯＳ等とのインタフェースである。通信制御１０３は、ＵＳＢコントローラ１５による通信動作を制御する。プロトコル制御１０４は、ＵＳＢのプロトコルに則って通信動作を管理・制御する。認証処理１０５は、プロトコル制御１０４の一部であり、後述の認証手順を担う。

【００１４】

ホスト２０のハードウエア構成については、ＰＣを初めとする情報処理装置の分野において常識的な構成であるため、特に説明しない。また、ホスト２０においても、アプリケーションプログラム２００がドライバ２０１を通じてＵＳＢを使用する、というソフトウエア構成が採られている。このドライバ２０１のモジュール構成は、ドライバ１０１のそれと同様である。但し、ドライバ２０１を構成する各モジュールの必須機能は、ドライバ１０１を構成する各モジュールの必須機能と、異なっている。この相違は、一つには、デバイス１０向けとホスト２０向けというインストール先の相違による相違や、インストール先のＯＳ等の相違による相違であり、いわゆる当業者であれば本願による開示から容易に推察できる。また、ドライバ１０１とドライバ２０１における対応モジュール間の機能上の相違は、また一つには、後述の諸機能を実現するための相違である。この相違については、いわゆる当業者であれば、本願による開示から、一意に理解できるであろう。

【００１５】

図３に、本実施形態における初期化手順を示す。この初期化手順は、デバイス１０がＵＳＢケーブルによりホスト２０に接続され、デバイス１０とホスト２０とがＵＳＢケーブルにより接続されたことが周知の手法により検出された直後に、ドライバ１０１とドライバ２０１との通信により実行される手順であり、本発明に係る初期化方法の好適な実施形態の一つである。この手順は、より詳細には、主としてプロトコル制御１０４及びその一部である認証処理１０５、並びにこれらに対応するドライバ２０１の構成モジュールにより、実行される。また、先にも述べたとおり、ＵＳＢにおける通常の初期化手順は、デバイス１０のコンフィギュレーションを示すコンフィギュレーションデータをデバイス１０からホスト２０に送信し、ホスト２０では受信したコンフィギュレーションデータの採否判断・選択を行い、その結果をデバイス１０に通知する処理を含んでいる。本実施形態における初期化手順でも、同様の処理を実行する。しかしながら、本実施形態における初期化手順は、図１２に示した初期化手順とは異なり、一般ユーザ向け即ちユーザモード用のコンフィギュレーションを示すコンフィギュレーションデータと特権ユーザ向け即ち特権モード用のコンフィギュレーションを示すコンフィギュレーションデータとを一括送信する、という処理を含んでいない。

【００１６】

即ち、本実施形態では、まずユーザモードに係るコンフィギュレーションデータが、デバイス１０（厳密にはそのドライバ１０１。以下同様）からホスト２０（厳密にはそのドライバ２０１。以下同様）へと送信される。ホスト２０が一般ユーザに係るホストである場合は、そのホスト２０は、このユーザモード用のコンフィギュレーションデータについてコンフィギュレーション選択を実行し、その結果をデバイス１０に通知する。ＵＳＢ通信開始許可を表す通知であれば、図３（Ａ）に示すように、ＵＳＢインタフェースによるデータ通信が開始される。ユーザモード用のコンフィギュレーションデータに基づく接続であることから、このデータ通信は、ユーザモードに係るコンフィギュレーションでの通信となる。この流れにおいては、特権モードに係るコンフィギュレーションデータは送信されないため、一般ユーザに係るホスト２０が初期化手順の実行を通じて特権モードの存在を知ることはない。

【００１７】

逆に、ホスト２０が特権ユーザに係るホストである場合は、そのホスト２０は、受信したコンフィギュレーションの内容如何によらず、図３（Ｂ）に示すように、デバイス１０に対して再コンフィギュレーションを要求する。再コンフィギュレーションの要求は、例えばベンダーコマンドへの割当のようにＵＳＢ規格に合致する方法の他、実用上差し障りがない場合は特権モード要求（図５参照）等のコマンドを追加するというＵＳＢ規格外の方法によっても、実行できる。再コンフィギュレーションの要求を受けたデバイス１０は、ホスト２０を相手として、デバイス１０・ホスト２０間の相互認証手順（或いは少なくともデバイス１０がホスト２０を認証する手順）を実行する。認証一致という結果が得られた場合に限り、デバイス１０は、ＵＳＢコントローラ１５に内蔵されるプルアップ抵抗を電気的にターンオンさせること等によって、ホスト２０側に、デバイス１０がホスト２０

から一旦切り離され再度接続されたかのように、認識させる。デバイス１０は、その上で、特権モードに係るコンフィギュレーションデータをホスト２０に送信し、ホスト２０は、これに応じてコンフィギュレーション選択を実行し、更にその結果に応じて、デバイス１０・ホスト２０間のデータ通信が開始される。特権モード用のコンフィギュレーションデータに基づく接続であることから、このデータ通信は、特権モードに係るコンフィギュレーションでの通信となる。

【００１８】

また、図３に示した手順では、ユーザモード及び特権モードという２種類のモードを想定していた。即ち、特権ユーザを全てひとくくりにしていた。これに対して、特権ユーザをレベル分けし、デバイス１０・ホスト２０間でやりとりできる情報の種別に関する制限の度合いを特権モードレベル毎に設定し、特権モードレベル毎にコンフィギュレーションを設定することも可能である。

【００１９】

仮に、特権ユーザのレベル即ち特権モードレベルが、低い方から順にレベル１、レベル２、　レベルＮの各レベルに分かれており（Ｎ：２以上の自然数）、接続先のホスト２０がレベルＩの特権ユーザに係るホストであるとする（Ｉ：１以上Ｎ以下の自然数）。この場合、例えば図４（Ａ）に示すように、ホスト２０が、再コンフィギュレーション要求に係るコマンド中に自分の特権モードレベルＩを示す情報をセットしてそのコマンドを送信する。デバイス２０は、認証一致と判断された後に、レベルＩの特権ユーザ向けのコンフィギュレーションを示すコンフィギュレーションデータを送信することによって、初期化手順を開始・再実行する。この手順では、ホスト２０の特権モードレベルが、認証前にデバイス１０側に知られる。

【００２０】

これに対して、図４（Ｂ）に示すように、特権モードレベルの昇順に従い、特権モードコンフィギュレーション送信／再コンフィギュレーション要求を繰り返す、という手順では、平均的に見れば図４（Ａ）よりも時間がかかるけれども、認証前にホスト２０の特権モードレベルがデバイス１０側に漏れることはなくなる。即ち、図４（Ｂ）に示した手順では、デバイス１０が、レベル１、レベル２、　という順で、最大でレベルＮまで、そのレベルに係る特権ユーザ向けのコンフィギュレーションを示すコンフィギュレーションデータを、送信する。ホスト２０では、自分の特権モードレベルに合致したコンフィギュレーションデータを受信した場合はそのコンフィギュレーションを選択し、そうでない場合は再コンフィギュレーションを要求する。ホスト２０がコンフィギュレーションを選択する旨をデバイス１０に通知した後、データ通信が開始される。

【００２１】

また、図４（Ａ）又は（Ｂ）に示した手順における再コンフィギュレーション要求を、特権モード要求等のＵＳＢ規格外コマンドに置き換えた図５（Ａ）又は（Ｂ）の手順によって、本発明を実施することもできる。図５（Ａ）に示した手順では、ホスト２０が特権モード要求に係るコマンド中に自分の特権モードレベルをセットして送信し、デバイス１０では認証一致後にこの特権モードレベルに対応したコンフィギュレーションデータによる初期化手順を開始・再実行する。図５（Ｂ）に示した手順では、ホスト２０が特権モード要求に係るコマンド中に自分の特権モードレベルをセットせずに送信し、デバイス１０では認証一致後に特権モードレベルの昇順に従いレベルＮまでを限度として各特権モードレベルに対応したコンフィギュレーションデータによる初期化手順を繰り返し実行する。

【００２２】

なお、図３～図５に示したいずれの手順においても、デバイス１０からホスト２０に特権モードレベルに関する通知を要求する等の動作は、実行されない。これは、一般ユーザに係るホスト２０に特権モードの存在を知られることを、防ぐためである。

【００２３】

認証手順は、例えば図６（Ａ）或いは（Ｂ）に示した手順により実行できる。図６（Ａ）に示したパターンによる認証手順では、デバイス１０からホスト２０への認証要求及びホ

スト２０からデバイス１０への認証応答に、それぞれデバイス１０又はホスト２０の認証コードが含まれており、それらの認証コードに基づきデバイス１０、ホスト２０又はその双方にて、双方の認証コード間に認証論理上の　　がないかどうかの判断即ち認証一致判断を行う（ホスト２０のみで一致判断を行う場合はその結果をホスト２０からデバイス１０に通知する）。図６（Ｂ）に示したパターンによる認証手順では、ホスト２０からの再コンフィギュレーション要求に係るコマンド中に、ホスト２０の認証コードが含まれている。また、図６（Ａ）における認証要求及び認証応答に代えて、それぞれ、デバイス１０の認証コードを含む認証応答と、ホスト２０における認証一致判断の結果を示す認証応答通知とが、送信される。いずれのパターンによるにしろ、認証一致であれば、前述の通り特権モードでの再接続のため特権モードに係るコンフィギュレーションデータにより初期化手順が実行され、認証不一致であれば、ホスト２０からの再コンフィギュレーション要求が正当なものでない等の可能性があるため、特権モードに係るコンフィギュレーションデータによる初期化手順は実行されない（切断状態となる）。なお、認証手順を別途並列的に実行することも可能である。

【００２４】

図７～図１１に、図３及び図６（Ａ）に示した手順を例として、ドライバ１０１及び２０１の動作の流れを示す。図７及び図８はドライバ１０１の、図９は一般ユーザに係るホスト２０のドライバ２０１の、図１０及び図１１は特権ユーザに係るホスト２０のドライバ２０１の、動作の流れである。デバイス１０がホスト２０に接続されそのことが認識されると（３００，４００）、ドライバ１０１によりユーザモード用のコンフィギュレーションデータが送信され（３０１）、そのデータがドライバ２０１により受信される（４０１）。ホスト２０が一般ユーザに係るホストである場合は、そのホスト２０のドライバ２０１によるコンフィギュレーション選択（４０２）の結果に応じて（３０２，３０３）、デバイス１０・ホスト２０間のデータ通信が開始される（３０４，４０３）。逆に、ホスト２０が特権ユーザに係るホストである場合は、そのホスト２０のドライバ２０１による再コンフィギュレーション要求（４０４）に応じて（３０２，３０３）、ドライバ１０１からの認証要求（３０５，４０５）及びドライバ２０１からの認証応答（４０６，３０６）を含む認証手順が実行され、ドライバ１０１側で認証一致判断を行う。このときドライバ２０１側では「切断」と認識しているため（４０７）、ドライバ１０１側で認証不一致と判断された場合はそのまま「切断」状態が続く（４０８）。これに対して、ドライバ１０１側で認証一致と判断されると、ドライバ１０１ではプルアップ抵抗ターンオン等により「再接続」状態に移行し（３０９）、ドライバ２０１はこれを以て「新規接続」と認識する（４０９）。その後、ドライバ１０１は特権モードに係るコンフィギュレーションデータを送信し（３１０，４１０）、ドライバ２０１はコンフィギュレーション選択を実行し（４１１，３１１）、しかる後、適宜、特権モードでのデータ通信が行われる（３１２，４１２）。

【００２５】

なお、以上の説明では、一般ユーザと特権ユーザとを想定していたが、本発明は、このような前提を必要とするものではない。即ち、本発明は、例えばハードウエア上の制約でコンフィギュレーションをいちどきに１種類しか送信できないデバイスから、ホストに対し複数通りのコンフィギュレーションを送信する手順としても、実施できる。

【００２６】

【発明の効果】

このように、本発明によれば、あるコンフィギュレーションについてホストからＵＳＢ通信開始拒否との通知を受けたデバイスが、先のコンフィギュレーションとは別のコンフィギュレーションにより初期化手順を再実行するようにしたため、特権ユーザ以外に特権モードの存在が察知されにくい形で特権モードを設けることや、ハードウエア等の制約でコンフィギュレーション送信が制限されているデバイスからの複数通りのコンフィギュレーション送信が、可能になる。例えば、まず一般ユーザ向けのコンフィギュレーションデータにより初期化手順を実行し、通信開始が拒否されたときは特権ユーザ向けのコンフィギ

ュレーションデータにより初期化手順を実行する、という手順によって、一般ユーザに係るホストに特権モードの存在を知られること、ひいては不必要な情報流出等の問題を防止・解消できる。また、特に特権モードでの接続に当たって、デバイスがホストを認証するため又はデバイス・ホスト間の相互認証のための認証手順を実行することにより、上掲の問題は更に少なくなる。また、本発明は、一般にＮ通り（Ｎ：２以上の自然数）のコンフィギュレーションを想定して実施すること、例えばＮ階層の特権モードレベルを各特権ユーザに付与して各特権モードレベル毎に異なるコンフィギュレーションによる接続とすることができる。そのための手順として、ホストからの特権モードレベル通知を含む手順だけでなく、デバイス側で最大Ｎ回に亘り初期化手順の再実行を繰り返す手順も採用できる。そして、本発明によれば、上掲の効果を、ドライバの改良によって達成できる。

【図面の簡単な説明】

【図１】本発明のハードウエア的実施環境例を示す図である。

【図２】本発明のソフトウエア的実施環境例を示す図である。

【図３】本発明の第１の実施形態における初期化手順を示す図であり、特に（Ａ）はホストが一般ユーザに係るホストであった場合を、（Ｂ）はホストが特権ユーザに係るホストであった場合を、それぞれ示すシーケンス図である。

【図４】本発明の他の実施形態に係る初期化手順を示す図であり、特に（Ａ）は第２の実施形態を、（Ｂ）は第３の実施形態を、それぞれ示すシーケンス図である。

【図５】本発明の他の実施形態に係る初期化手順を示す図であり、特に（Ａ）は第４の実施形態を、（Ｂ）は第５の実施形態を、それぞれ示すシーケンス図である。

【図６】本発明の好適な実施形態における認証手順の例を示す図であり、特に（Ａ）は認証要求／認証応答による手順を、（Ｂ）は再コンフィギュレーション／認証応答／認証応答通知による手順を、それぞれ示すシーケンス図である。

【図７】本発明の第１の実施形態におけるデバイス側のドライバの動作の流れのうち前半を示すフローチャートである。

【図８】本発明の第１の実施形態におけるデバイス側のドライバの動作の流れのうち後半を示すフローチャートである。

【図９】本発明の第１の実施形態におけるホスト側のドライバの動作の流れ、特に一般ユーザに係るホストにおける流れを示すフローチャートである。

【図１０】本発明の第１の実施形態におけるホスト側のドライバの動作の流れ、特に特権ユーザに係るホストにおける流れの前半を示すフローチャートである。

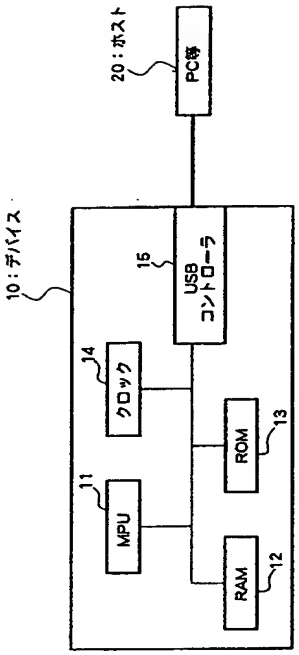
【図１１】本発明の第１の実施形態におけるホスト側のドライバの動作の流れ、特に特権ユーザに係るホストにおける流れの後半を示すフローチャートである。

【図１２】従来技術の単純変形による初期化手順を示す図であり、特に（Ａ）はホストが一般ユーザに係るホストであった場合を、（Ｂ）はホストが特権ユーザに係るホストであった場合を、それぞれ示す図である。

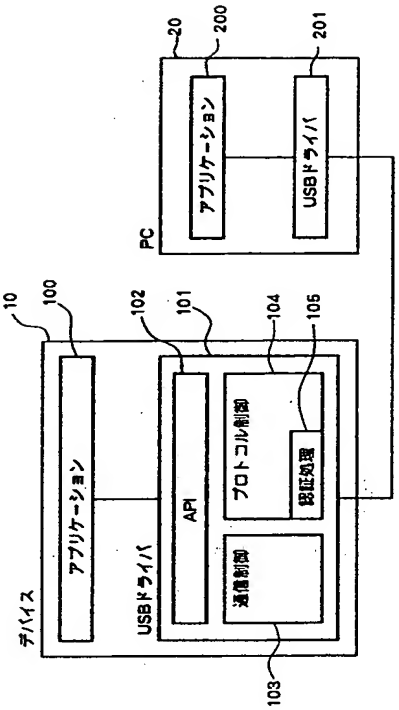
【符号の説明】

１０　デバイス、１０１．２０１　ドライバ、１０４　プロトコル制御、１０５　認証処理、２０　ホスト。

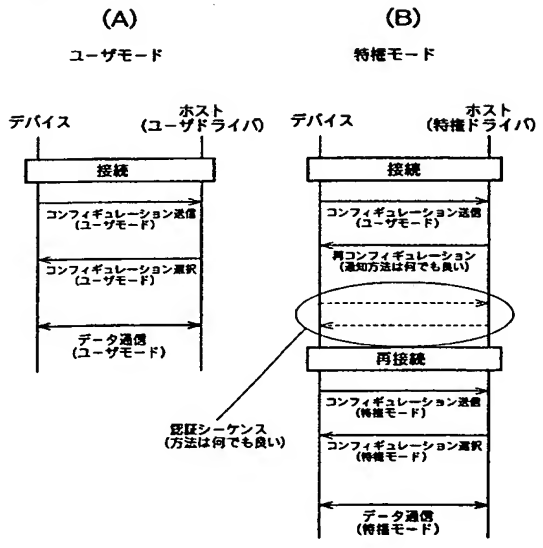
【図１】


20：ホスト
PC等
10：デバイス
15
USB
コントローラ
14
クロック
ROM
13
11
MPU
RAM
12

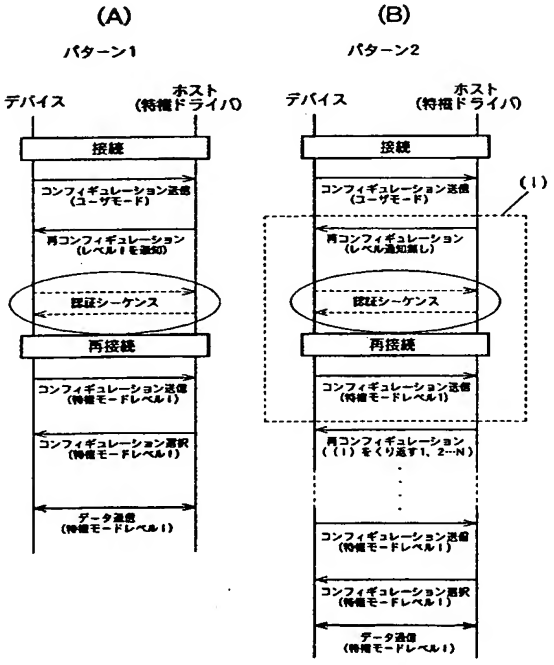
【図２】


20
200
201
アプリケーション
USBドライバ
PC
10
100
102
101
104
105
アプリケーション
API
プロトコル制御
認証処理
通信制御
USBドライバ
デバイス
103

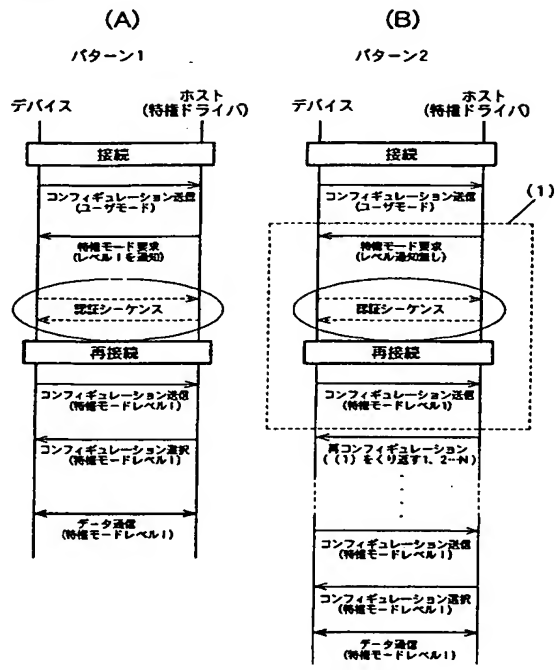
【図３】


(A)
ユーザモード
(B)
特権モード
デバイス
ホスト
(ユーザドライバ)
デバイス
ホスト
(特権ドライバ)
接続
コンフィギュレーション送信
(ユーザモード)
コンフィギュレーション選択
(ユーザモード)
データ通信
(ユーザモード)
接続
コンフィギュレーション送信
(ユーザモード)
再コンフィギュレーション
(通知方法は何でも良い)
認証シーケンス
(方法は何でも良い)
再接続
コンフィギュレーション送信
(特権モード)
コンフィギュレーション選択
(特権モード)
データ通信
(特権モード)

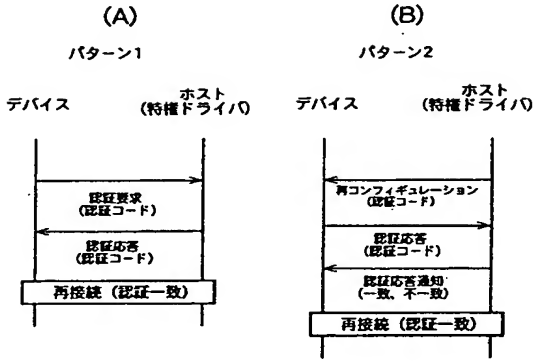
【図４】


(A)
パターン1
(B)
パターン2
デバイス
ホスト
(特権ドライバ)
デバイス
ホスト
(特権ドライバ)
接続
コンフィギュレーション送信
(ユーザモード)
再コンフィギュレーション
(レベル1を通知)
認証シーケンス
再接続
コンフィギュレーション送信
(特権モードレベル1)
コンフィギュレーション選択
(特権モードレベル1)
データ通信
(特権モードレベル1)
接続
コンフィギュレーション送信
(ユーザモード)
(1)
再コンフィギュレーション
(レベル通知無し)
認証シーケンス
再接続
コンフィギュレーション送信
(特権モードレベル1)
再コンフィギュレーション
((1)をくり返す1, 2…N)
コンフィギュレーション送信
(特権モードレベル1)
コンフィギュレーション選択
(特権モードレベル1)
データ通信
(特権モードレベル1)

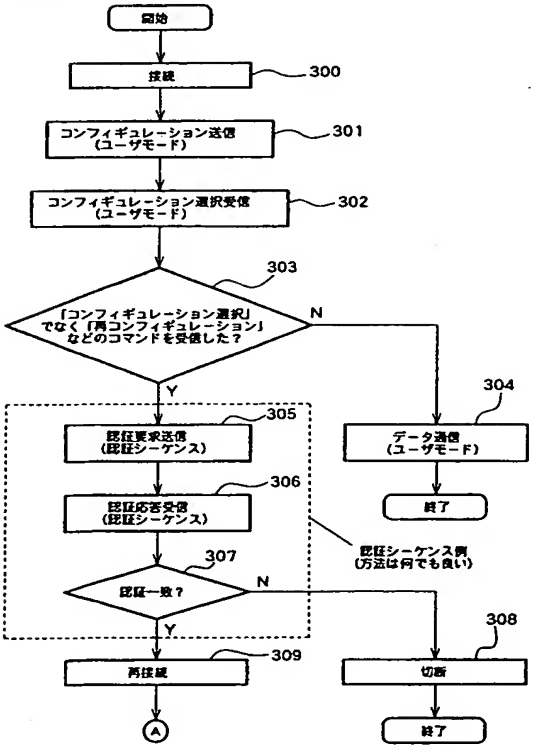
【図５】


(A)
パターン1
(B)
パターン2
デバイス
ホスト
(特権ドライバ)
接続
コンフィギュレーション送信
(ユーザモード)
特権モード要求
(レベル1を通知)
特権モード要求
(レベル通知無し)
認証シーケンス
再接続
コンフィギュレーション送信
(特権モードレベル1)
コンフィギュレーション選択
(特権モードレベル1)
データ通信
(特権モードレベル1)
(1)
再コンフィギュレーション
((1)をくり返す1, 2…N)

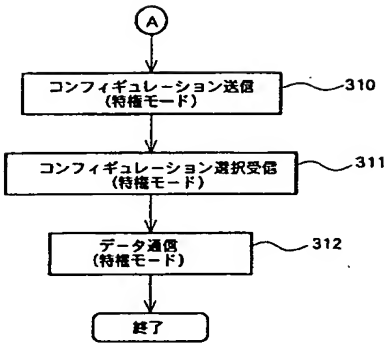
【図６】


(A)
パターン1
(B)
パターン2
デバイス
ホスト
(特権ドライバ)
認証要求
(認証コード)
認証応答
(認証コード)
再接続（認証一致）
再コンフィギュレーション
(認証コード)
認証応答
(認証コード)
認証応答通知
(一致、不一致)
再接続（認証一致）

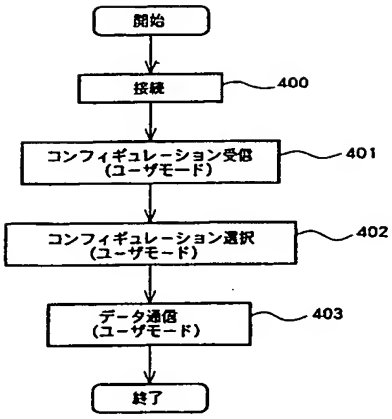
【図７】


開始
接続
300
コンフィギュレーション送信
(ユーザモード)
301
コンフィギュレーション選択受信
(ユーザモード)
302
303
「コンフィギュレーション選択」
でなく「再コンフィギュレーション」
などのコマンドを受信した？
N
Y
304
データ通信
(ユーザモード)
終了
305
認証要求送信
(認証シーケンス)
306
認証応答受信
(認証シーケンス)
認証シーケンス例
(方法は何でも良い)
307
認証一致？
N
Y
308
切断
終了
309
再接続
A

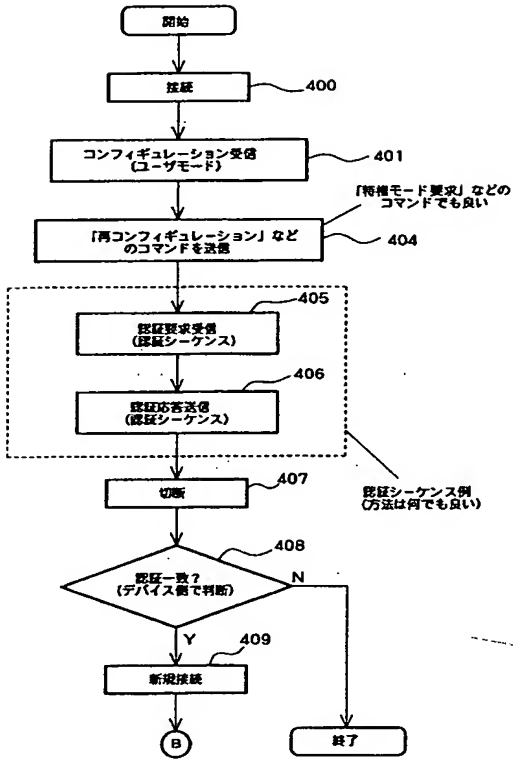
【図８】


A
コンフィギュレーション送信
(特権モード)
310
コンフィギュレーション選択受信
(特権モード)
311
データ通信
(特権モード)
312
終了

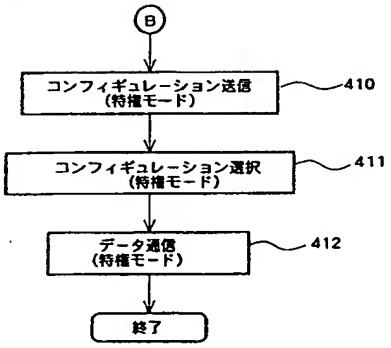
【図９】



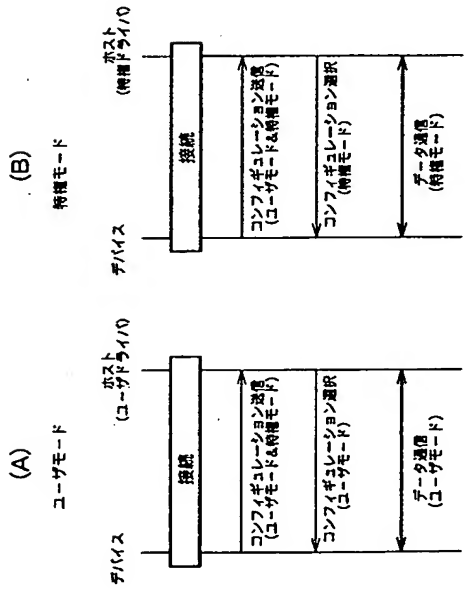
【図１０】



【図１１】



【図１２】



フロントページの続き

(72)発明者 鈴木 正則
東京都三鷹市下連雀五丁目１番１号 日本無線株式会社内
(72)発明者 森本 真史
東京都三鷹市下連雀五丁目１番１号 日本無線株式会社内
(72)発明者 塩原 徹也
東京都三鷹市下連雀五丁目１番１号 日本無線株式会社内

Ｆターム(参考) 5B014 FB04 HC05
5B077 NN02